CyberEco

معًا لدَعْم السَّلامة الرَّقميَّة

Together to support digital safety

حمـاية الأجـهزة الإلكترونيَّة ومُواجَـهة الاختراقات الأمنيَّة

محتوى تدريبيّ موجَّه لأولياء الأمور

شرائح العَرْض

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

حُقُوق المِلْكِيَّة الفِكْرِيَّة

ديسمبر 2023م

الدوحة، قطر

هذا المحتوى إنتاج فريق

إدَارة التَّميُّز السّيبرانيّ الوَطنيّ، الوكالة الوطنيَّة للأَمْن السّيبرانيّ.

للاستفسار عن المُبادَرة أو البرنامج؛ يمكن التَّواصُل عن طريق المواقع الإلكترونيَّة أو الأرقام الهاتفيَّة التَّالية:

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

https://www.ncsa.gov.qa/
cyberexcellence@ncsa.gov.qa
00974 404 663 78
00974 404 663 62

التَّوزيع الزَّمنيّ للوَرشَة

المحتوى	الوقت المُخصَّص
تمهيد	5 دقائق
الجُزْء النَّظريّ من المادَّة	25 دقيقة
عَرْض الفيديوهات التَّعليميَّة	25 دقيقة
استراحة قصيرة	20 دقيقة
تنفيذ الأَلْعَاب التَّدريبيَّة	25 دقيقة
حِوَار ونِقَاش مع الطَّلَبة	15 دقيقة
مَشروع التَّخرُّج	5 دقائق
المُدَّة الزَّمنيَّة للورشَة	ساعتان

فهرس المحتوى العِلْمِيّ

الفَصْل الأوّل
أهمّيّة أمن الأجهزة الإلكترونيّة والشّبكات

أوّلًا

أهمّيّة الاستقرار الرّقميّ بالنّسبة للشّبكات وللأجهزة المُتّصلة بها

أمـن المعلومـات
Security Information

يُقصَد به الوسائل والأدوات والإجراءات اللَّازم توفيرها لضمان حماية المعلومات من الأخطار الدَّاخليَّة والخارجيَّة، وهو العِلْم الذي يَدْرُس كيفيَّة توفير تدابير حماية سرِّيَّة وسالمة للمعلومات وكيفيَّة مكافحة الاعتداء عليها.

تقوم حماية المعلومات على عدَّة خطوات تضمن حماية الأجهزة والشَّبكات من الاختراق، وهي:

01 استخدام اسم المُستخدِم وكلمة المرور.

02 حماية الحاسوب من المُتسلِّلين عبر برامج مكافحة الفيروسات.

03 حماية البرامج والبيانات والنَّسْخ الاحتياطيّ.

04 استخدام جدار الحماية Firewall.

أمـن الشَّبكـات

هو جزء من منظومة أمن المعلومات التي تقوم على حماية استخدام الشَّبكة وسلامتها ومن ثمّ سلامة البيانات، ويشمل هذا المجال كلًّا من تكنولوجيا الأجهزة والبرمجيَّات، ويَستهدِف مجموعةً مُتنوِّعةً من التَّهديدات ويَمْنَعُها من الدُّخول إلى شبكتك أو من الانتشار.

أساسيَّات أمن الشَّبكات

- التَّحكُّم في الوصول: ويُقصَد به فَرْض سياسات أمان تَمْنَع المُستخدِمين غير المُصرَّح لهم باستخدام شبكتك من الدُّخول إليها ومن ثمّ من الوصول إلى أجهزتك وبياناتك، ويُطْلَق على هذه العمليَّة "التَّحكُّم في الوصول إلى الشَّبكة" network access control.
- برامج مُكَافَحَة الفيروسات والبرمجيَّات الخبيثة.
- أمان التَّطبيقات.

- التَّحليل السُّلوكيّ: إذ تقوم أدوات التَّحليل السُّلوكيّ بالتَّمييز التِّلقائيّ للأنشطة التي يُشْتَبه فيها لمعالجتها سريعًا.
- الحماية من فقدان البيانات.
- أمان البريد الإلكترونيّ.
- جدران الحماية.
- أنظمة مَنْع التسلل.
- أمان الجهاز المحمول.
- تقسيم الشَّبكة.
- أمن الويب.

المَخاطِر الرَّقميَّة التي تواجه الأجهزة الرَّقميَّة (الحواسيب، الهواتف الذَّكيَّة، الأجهزة اللَّوحيَّة)

01 تَسَـــرُّب البيانـــات

في بعض الأحيان تكون تطبيقات الأجهزة المحمولة سببًا في تَسَرُّب البيانات غير المُتعمَّد، فعلى سبيل المثال، تمثل التطبيقات المُصنَّفة كبرمجيَّات خطرة -والتي تأتي مجانية- مشكلة حقيقيَّةً لمُستخدِمي الأجهزة المحمولة الذين يمنحونها أذوناتٍ شاملةً دون التَّحقُّق من الأمن دائمًا.

02 تزويـــر الشَّبكـــة

عادةً ما تكون شبكات Wi-Fi المجانيَّة أو (العامَّة) غير آمِنة، ولكي يكون المُستخدِم بمأمن من الهجمات الإلكترونيَّة عليه ألَّا يَستخدِم شبكة Wi-Fi المجانيَّة على جهازه المحمول إلَّا نادرًا، ولا يَستخدِمها مطلقًا للوصول إلى الخدمات السِّرِّيَّة أو الشَّخصيَّة، مثل المعلومات المصرفيَّة أو معلومات بطاقات الائتمان.

المَخاطِر الرَّقميَّة التي تواجه الأجهزة الرَّقميَّة (الحواسيب، الهواتف الذَّكيَّة، الأجهزة اللَّوحيَّة)

03 هجمات التَّصيُّد الاحتياليّ

يُعَدّ مُستخدِمو الأجهزة المحمولة الأكثر عرضةً للهجمات؛ لأنَّهم غالبًا ما يكونون أوَّل مستلمي رسائل البريد الإلكترونيّ التي تبدو شرعيَّة ويلتقطون الطُّعم؛ لذا يجب عدم النَّقْر مطلقًا فوق روابط البريد الإلكترونيّ غير المألوفة.

04 برمجيَّات التَّجسُّس

يجب تنزيل مجموعة برامج فعَّالة لمُكَافَحَة الفيروسات وكَشْف البرمجيَّات الضَّارَّة؛ للمساعدة على كَشْف هذه البرمجيَّات والتَّخلُّص منها قبل أن تُتاح لها فرصة جَمْع البيانات الشَّخصيَّة.

الفَصْل الثَّاني
أنواع المَخاطِر الرَّقميَّة التي تواجه الأجهزة

هجوم الفِدْيَة

عبارة عن برمجيَّات ضارَّة مُصمَّمة لمَنْع المُستخدِم أو المؤسَّسة من الوصول إلى الملفَّات الموجودة على أجهزة الحاسوب الخاصَّة بهم، للمُطالَبَة بدَفْع فِدْيَة مقابل استعادة الوصول إلى ملفَّاتهم.

كيفيَّة عمل برمجيَّات الفِدْيَة

ناقلات العدوى والتَّوزيـع

يميل مُشغِّلو برمجيَّات الفِدْيَة إلى استخدام رسائل البريد الإلكترونيّ التَّصيُّديَّة؛ فقد تحتوي رسالة البريد الإلكترونيّ الضَّارَّة على رابط إلى موقع ويب يستضيف تنزيلًا ضارًّا أو مُرفَقًا ضارًّا.

تشفيـر البيانـات

بمجرَّد أن يتمكَّن مجرمو الإنترنت من الوصول إلى نظام الحاسوب سواء للفرد أم للمؤسَّسة؛ يبدأ النِّظام تشفير ملفَّاته واستبدال النُّسَخ الأصليَّة بالإصدارات المُشفَّرة للمساومة عليها فيما بعد.

طلـب الفِدْيَـة

بعد اكتمال تشفير الملفَّ يصبح برنامج الفِدْيَة جاهزًا لتقديم طَلَب فِدْيَة.

أساسيَّات أمن الشَّبكات

- التَّدريب والتَّعليم للتَّوعية السِّيبرانيَّة.
- النَّسْخ الاحتياطيّ المستمرّ للبيانات.
- تصحيح الثَّغرات في الأنظمة التي لم تُصحَّح بعد.
- تُعَدّ مصادقة المُستخدِم وسيلةً مهمَّةً لمَنْع المُهاجِم من الاستفادة من كلمة المرور التي تمّ تخمينها أو سرقتها.
- تقليل سَطْح الهجوم، ويتمّ ذلك عن طريق معالَجة الآتي:

رسائل التَّصيُّد	نقاط الضَّعف غير المُصحَّحة
حلول الوصول عن بُعْد	البرمجيَّات الضَّارَّة للهواتف الذَّكيَّة

كيفيَّة التَّخفيف من عدوى برمجيَّات الفِدْيَة النَّشطة

01

عَزْل الجهاز

يجب قَطْع الطَّريق أمام البرمجيَّات الخبيثة عبر عَزْل الجهاز الذي تَلَقَّى رسالة الفِدْيَة عن باقي الأجهزة المُتَّصلة به.

02

تَرْك الحاسوب قَيْد التَّشغيل

يؤدِّي تشفير الملفَّات إلى جَعْل الحاسوب غير مستقرّ، لذا فإنّ إيقاف تشغيل الحاسوب ليس الحلّ الأكمل؛ لأنَّه قد يؤدِّي إلى فقدان الذَّاكرة.

03

إنشاء نسخة احتياطيَّة من الملفَّات.

04

التَّحقُّق من وجود أدوات فكّ التَّشفير

تَحَقَّق من مشروع No More Ransom Project لمعرفة ما إذا كان برنامج فكّ التَّشفير المجانيّ متاحًا أم لا؛ ليساعدك على استعادة الملفَّات.

05

اطْلُب المساعدة

يمكن أن يساعد شخص مُتخصِّص في استعادة هذه النُّسَخ إذا لم يتمّ حَذْفها بواسطة البرمجيَّات الضَّارَّة.

06

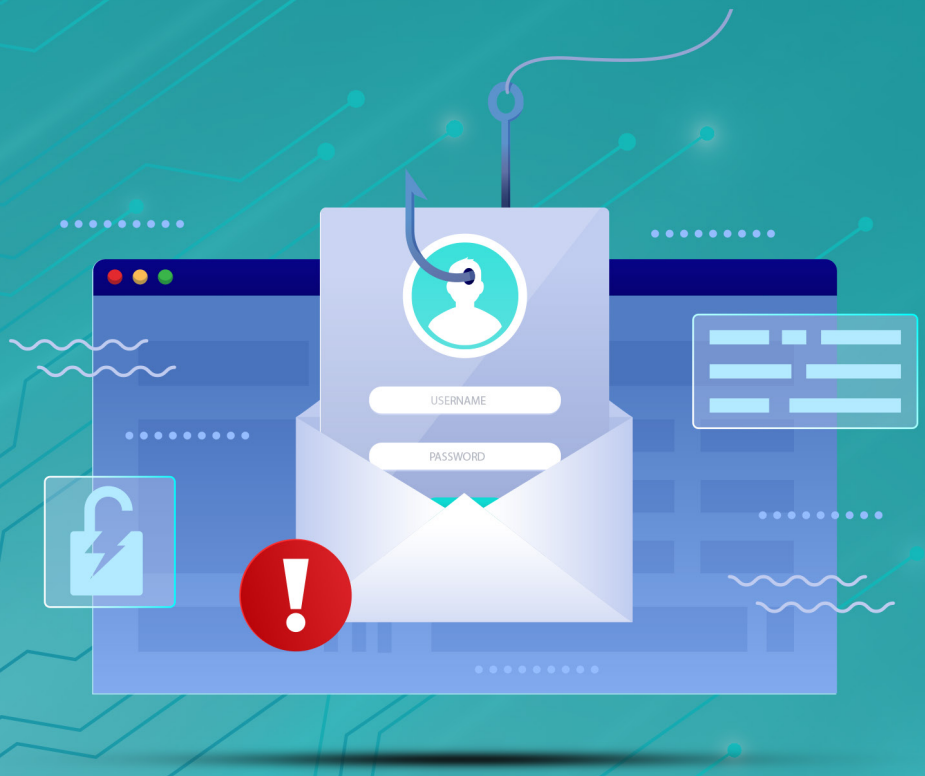
المَسْح والاستعادة

يجب استعادة الجهاز من نسخة احتياطيَّة نظيفة أو تثبيت نظام التَّشغيل؛ لضمان إزالة البرمجيَّات الضَّارَّة بالكامل من الجهاز.

سرقة بيانات الأجهزة

تعريف سرقة البيانات

هي نَقْل أو تَخْزين غير قانونيّ للمعلومات الشَّخصيَّة أو السِّرِّيَّة أو الماليَّة، ويمكن أن يشمل ذلك كلمات المرور أو التَّعليمات البرمجيَّة أو الخوارزميَّات البرمجيَّة والعمليَّات أو التِّقنيَّات الخاصَّة، وتُمثِّل انتهاكًا خطيرًا للأمان والخصوصيَّة.



يُطْلَق على سرقة البيانات أيضًا المُصْطَلَحان "خَرْق البيانات" و"تَسَرُّب البيانات"، لكنَّ هناك فروقًا بسيطة بينهما:

01 يحدث تَسرُّب البيانات

عندما يتمّ الكَشْف عن بيانات حسَّاسة عن طريق الخطأ، إمَّا على الإنترنت وإمَّا من خلال مُحرِّكات الأقراص الثَّابتة أو الأجهزة المفقودة، أي يمكن لمخترقي البيانات الوصول غير المُصرَّح به إلى البيانات الحسَّاسة دون جهد منهم.

02 يُشير خَرْق البيانات

إلى الهجمات الإلكترونيَّة المُتعمَّدة.

كيف تحدث سرقة البيانات؟

1. **الهندسة الاجتماعيَّة** الشَّكل الأكثر شيوعًا لها هو التَّصيُّد الاحتياليّ، ويحدث عندما يَتَنَكَّر المُهاجِم في صورة كيان موثوق به؛ لِخِدَاع الضَّحيَّة لفَتْح بريد إلكترونيّ أو رسالة نصيَّة أو رسالة فوريَّة.

2. **كلمات المرور الضَّعيفة.**

3. **نقاط ضعف النِّظام**
تُساعِد الثَّغرات الأمنيَّة المُتسلِّلين في استغلالها لسرقة البيانات، وتؤدِّي برامج مُكَافَحَة الفيروسات القديمة أيضًا إلى إنشاء ثغرات أمنيَّة.

4. **التَّهديدات الدَّاخليَّة**
يمكن للمُوظَّفين الذين يعملون في مؤسَّسةٍ ما الوصول إلى المعلومات الشَّخصيَّة للعملاء واستغلالها.

كيف تحدث سرقة البيانات؟

5 **الخطأ البشريّ** وهو إرسال معلومات حسَّاسة إلى الشَّخص الخطأ، مثل إرسال بريد إلكترونيّ عن طريق الخطأ إلى عنوان غير صحيح، أو تسليم ملفٍّ فِعْليٍّ إلى شخص لا ينبغي له الوصول إلى المعلومات.

6 **تثبيت البرامج من مواقع غير آمِنة** قد يقوم أحد الأشخاص بتنزيل برامج أو بيانات من مواقع الويب المُختَرَقة والمصابة بفيروسات.

7 **سرقة الأجهزة الإلكترونيَّة أو فُقدانها.**

8 **المعلومات المتاحة للجمهور** يمكن العثور على كثير من المعلومات من خلال عمليَّات البَحْث على الإنترنت والبَحْث في منشورات المُستخدِمين على الشَّبكات الاجتماعيَّة.

ما أنواع البيانات التي تتمّ سرقتها عادةً؟

1. سجلّات العملاء.
2. البيانات الماليَّة، مثل معلومات بطاقة الائتمان أو بطاقة الخَصْم.
3. رموز المصدر والخوارزميّات.
4. أوصاف عمليَّة الملكيَّة ومنهجيَّات التَّشغيل.
5. بيانات اعتماد الشَّبكة، مثل أسماء المُستخدِمين وكلمات المرور.
6. سجلّات الموارد البشريَّة وبيانات المُوظَّفين.
7. المستندات الخاصَّة المُخزَّنة على أجهزة الحاسوب.

عواقب سرقة البيانات

1. الدَّعاوى القضائيَّة المُحتمَلة من العملاء الذين تمّ الكَشْف عن معلوماتهم.
2. طَلَبات الفِدْيَة من المُهاجِمين.
3. تكاليف الاسترداد، على سبيل المثال، استعادة أو تصحيح الأنظمة التي تمّ خرقها.
4. الإضرار بالسُّمعة وخسارة العملاء.
5. الغرامات أو العقوبات من الهيئات التَّنظيميَّة حَسْب الصِّناعة.
6. التَّوقُّف في أثناء استعادة البيانات.
7. بالنِّسبة للأفراد الذين تمّ خرق بياناتهم، فإنَّ النَّتيجة الرَّئيسة هي أنّ ذلك قد يؤدِّي إلى سرقة الهُوِيَّة؛ ما يُسبِّب لهم خسارةً ماليَّةً واضطرابًا عاطفيًّا.

كيفيَّة الحفاظ على البيانات آمِنة

1. اسْتَخدِم كلمات مرور قويَّة وغيِّرها من حين إلى آخر.
2. تَجَنَّب استخدام نفس كلمة المرور لحسابات مُتعدِّدة.
3. تَجَنَّب كتابة كلمات المرور الخاصَّة بك في أيّ مكان.
4. المصادقة مُتعدِّدة العوامل.
5. كُن حَذِرًا عند مشاركة المعلومات الشَّخصيَّة.
6. الحد من مشاركة البيانات الشَّخصيَّة عَبْر منصَّات التواصل الاجتماعيّ.
7. إغلاق الحسابات غير المُستخدَمة على الإنترنت.
8. حافِظ على تحديث الأنظمة والبرامج.
9. كُن حَذِرًا من خدمة Wi-Fi المجانيَّة.
10. اسْتَخدِم برامج مُكَافَحَة الفيروسات.

الوصول غير القانونيّ

الوصول غير المُصرَّح به (غير القانونيّ) هو عمليَّة الدُّخول إلى موارد الحاسوب دون إذْنٍ، ويمكن أن يكون نظامًا أو شبكةً أو برنامجًا أو بياناتٍ، وعادةً ما يتمّ ارتكاب الوصول غير المُصرَّح به من قِبل المُتسلِّلين، وأحيانًا المُستخدِمين غير المُتعمِّدين، فيمكن لأيّ شخص لديه إمكانيَّة الوصول بالفعل إلى النِّظام أن يَعْثُر بطريق الخطأ على ملفَّات غير آمِنة لم تكن مُخصَّصة للمُعاينة.

كيفيّة وصول الأشخاص غير المُصرّح لهم إلى الأنظمة والملفّات

1

تخمين المُستخدِم -عن طريق الخطأ- كلمة مرور لملفّات أو بيانات حسّاسة.

2

تنفيذ هجمات مُعقّدة تستغرق أسابيع من التّخطيط، وقد تتضمّن حتى تجسُّسًا على المؤسّسات والمُستخدِمين.

3

يمكن لمخترقي البيانات أن يذهبوا إلى أبعد من ذلك في خداعهم لاكتساب ما يكفي من الثّقة ليكونوا أشخاصًا مُرخّصًا لهم.

مَخاطِر الوصول غير المُصرَّح به

1. تعطيل الأنظمة الإلكترونيَّة.
2. إيذاء الهدف؛ فعادةً ما تكون البيانات غير المُصرَّح بها حسَّاسة ويمكن أن تُلْحِق الضَّرر بالصَّحيَّة.
3. سرقة البيانات للحصول على فِدْيَة.
4. يُسبِّب أضرارًا ماديَّة للأجهزة المُتَّصلة بالشَّبكة.
5. الإضرار بسمعة المؤسَّسات والأفراد.
6. العقوبات الماليَّة والمعنويَّة على المؤسَّسات لتَعَرُّض العملاء للضَّرر.
7. تزايد التَّكاليف نتيجة إصلاح الثَّغرات والأعطال النَّاتجة عن الوصول غير المُصرَّح به للأنظمة والملفَّات، ودَفْع التَّعويضات للمتضرِّرين.

نصائح لاكتشاف الدُّخول غير المُصرَّح به ومَنْعه

01

وَضْع كلمة مرور قويَّة ومُعقَّدة وتغييرها من حين إلى آخر.

02

التَّذكير والفحوص المُنتظِمة بشأن الممارسات الأمنيَّة عبر التَّدريب.

03

تقليل عدد الأجهزة التي يمكنها الوصول إلى البيانات الحسَّاسة.

04

تأمين جميع نقاط النِّهاية عبر تثبيت برنامج مُكَافَحَة الفيروسات على كلّ نقطة نهاية؛ لاكتشاف البرمجيَّات الضَّارَّة وإزالتها.

البرمجيَّات الضَّارَّة

البرمجيَّات الضَّارَّة مصطلح شامل يَصِف أيّ برنامج أو تعليمات برمجيَّة ضارَّة تَضُرّ بالأنظمة، فهي تسعى عن عَمْد إلى غَزْو أجهزة الحاسوب وأنظمتها والشَّبكات والأجهزة اللَّوحيَّة والأجهزة المحمولة بهدف إتلافها أو تعطيلها، وذلك غالبًا عن طريق التَّحكُّم الجزئيّ في عمليَّات الجهاز.

علامات إصابة الجهاز بالبرمجيَّات الضَّارَّة

- بُطْء جهاز الحاسوب الخاصّ بك.
- ظهور الإعلانات المُنبثقة المُزعِجة على الشَّاشة.
- تَعَطُّل النِّظام الخاصّ بك، ويأتي هذا على شكل تجميد أو شاشة الموت الزَّرقاء (BSOD)، ويحدث هذا الأخير على أنظمة Windows بعد مواجهة خطأ فادح.
- فقدانٌ غامضٌ لمساحة القُرْص.
- زيادة غريبة في نشاط الإنترنت لنظامك.
- تَغَيُّر إعدادات المُتصفِّح الخاصّ بك.
- تَوقُّف برنامج مُكَافَحَة الفيروسات الخاصّ بك عن العمل، ولا يعود بإمكانك تشغيله مرَّةً أخرى.
- فقدان إمكانيَّة الوصول إلى ملفَّاتك أو جهاز الحاسوب بأكمله.

أنواع البرمجيَّات الضَّارَّة

1. برمجيَّات الإعلانات المُتسلِّلة
2. برمجيَّات التَّجسُّس
3. الفيروسات
4. ديدان الحاسوب
5. حصان طروادة
6. برمجيَّات الفِدْيَة
7. برمجيَّات الاستغلال

كيفيَّة إزالة البرمجيَّات الضَّارَّة

خطوات إزالة البرمجيَّات الضَّارَّة

1. ثَبِّت وحَمِّل برنامجًا جيِّدًا لمُكافَحة البرمجيَّات الضَّارَّة.

2. أجْرِ فَحْصًا باستخدام برنامجك الجديد.

3. غَيِّر جميع كلمات المرور الخاصَّة بك.

كيفيَّة الحماية من البرمجيَّات الضَّارَّة

- انْتَبِه إلى النِّطاق وكُن حَذِرًا إذا لم يكُن الموقع نطاقًا من المستوى الأعلى، مثل com أو mil أو net أو org أو edu أو biz، على سبيل المثال لا الحصر.
- اسْتَخدِم كلمات مرور قويَّة مع مصادقة مُتعدِّدة العوامل.
- تَجَنَّب النَّقْر على الإعلانات المُنبثِقة في أثناء تَصَفُّح الإنترنت.
- تَجَنَّب فَتْح مُرْفَقات البريد الإلكترونيّ من مُرسِلِين غير معروفين.
- لا تَنْقُر على الرَّوابط الغريبة.
- لا تقم بتحميل البرامج والتَّطبيقات من المواقع غير الموثوقة.

- الْتَزِم بالتَّطبيقات الرَّسميَّة من App Store وGoogle Play.
- تأكَّد من أنّ نظام التَّشغيل والمُتصفِّحات والمُكوِّنات الإضافيَّة لديك مُصحَّحة ومُحدَّثة.
- احْذِف أيّ برامج لم تَعُد تستخدمها.
- قُمْ بعمل نسخة احتياطيَّة لبياناتك بانتظام.
- ثَبِّت برنامجًا حديثًا على جهازك لمكافحة الفيروسات والبرمجيات الضَّارَّة.

الفَصْل الثَّالث
حماية الأجهزة من الأخطار الرَّقميَّة

كلمـات المـــرور

ما استخدام الحماية بكلمة المرور؟

تُساعِد الحماية بكلمة مرور على حماية بياناتك من الجِهات الفاعلة السَّيِّئة، من خلال اكتشاف كلمات المرور الضَّعيفة المعروفة والمصطلحات الضَّعيفة الخاصَّة بك وحَظْرها، فهي تقنيَّة للتَّحكُّم في الوصول تُساعِد في الحفاظ على البيانات المهمَّة آمِنةً من المُتسلِّلين، من خلال ضمان عدم إمكانيَّة الوصول إليها إلَّا باستخدام بيانات الاعتماد الصَّحيحة.

أهمِّيَّة حماية كلمة المرور

هي خطّ الدِّفاع الأوَّل ضدّ الوصول غير المُصرَّح به إلى الحسابات والأجهزة والملفَّات عبر الإنترنت، وتُساعِد كلمات المرور القويَّة على حماية البيانات من العناصر السَّيِّئة والبرمجيَّات الضَّارَّة، فكلَّما كانت كلمة المرور أقوى؛ زادت حماية المعلومات.

عواقب استخدام كلمات المرور الضَّعيفة

بالنِّسبة للأفراد، يمكن أن يكون لفقدان المعلومات الشَّخصيَّة تداعيات ماليَّة وتداعيات على السُّمعة طويلة الأمد.

وعندما يحصل مخترقو البيانات على وصول غير مُصرَّح به إلى بيانات المؤسَّسة، يمكن أن تَتَعَرَّض إلى خسارة كبيرة في الإيرادات والمِلْكِيَّة الفِكْرِيَّة وتعطيل العمليَّات، فضلًا عن تَكَبُّد غرامات تنظيميَّة والإضرار بالسُّمعة.

إرشادات عامَّة لإنشاء كلمات مرور قويَّة

1. اسْتَخدِم ما لا يقلّ عن 12 حرفًا.
2. اسْتَخدِم مزيجًا من الحروف والأرقام والرُّموز.
3. اسْتَخدِم حرفًا كبيرًا واحدًا على الأقلّ.
4. اسْتَخدِم كلمة مرور مختلفة لكلّ حساب من حساباتك.
5. اسْتَخدِم كلمات غير مألوفة وغير عاديَّة، مثل كلمات الأغاني أو الاقتباسات أو العبارات الشَّائعة.


بعض الأمثلة على كلمات المرور الضّعيفة
1
1234567
2
1111111
3
كلمة المرور 123

النَّسْخ الاحتياطيّ للبيانات

إستراتيجيَّات فعَّالة لإجراء نَسْخ احتياطيّ آمِن لبياناتك

- **قاعدة 3-2-1، ويُقصَد بها إنشاء 3 نُسَخ مختلفة من بياناتك لوَضْعها على نوعين مختلفين من وحدات التَّخزين والاحتفاظ بنسخة واحدة خارج الموقع، وهناك عدَّة طُرق لذلك:**
  - استخدام مُحرِّك أقراص ثابت خارجيّ.
  - استخدام برنامج نَسْخ احتياطيّ تابِع لجهة خارجيَّة، مثل البرامج السَّحابيَّة.
  - نَسْخ الملفَّات يدويًّا.

- اسْتَخدِم مُحرِّك أقراص فلاش USB.
- اسْتَخدِم الوسائط البصريَّة، مثل الأقراص المضغوطة أو أقراص DVD، لعمل نسخة من بياناتك.
- اسْتَخدِم التَّخزين السَّحابيّ، مثل: Backb، Dropbox، iCloud، Google Drive.
- اسْتَخدِم خدمة النَّسْخ الاحتياطيّ عبر الإنترنت.
- اسْتَخدِم جهاز تخزين متَّصل بالشَّبكة (NAS): هو خادم مُخصَّص يُوفِّر تخزينًا ومشاركة على مستوى الملفّ لشبكة منزلك أو شركتك الصَّغيرة، وهو قَيْد التَّشغيل والاتِّصال دائمًا؛ حتى تتمكَّن من الوصول إلى بياناتك في أيّ وقت ومن أيّ مكان.


البطاقات التّدريبيّة

انْتَبِه!

جهاز التخزين (NAS)

هو جِهاز مُخصَّص يُوفِّر تخزينًا ومشاركة على مستوى الملفّ لشبكة منزلك أو شركتك الصَّغيرة، وهو قَيْد التَّشغيل والاتِّصال دائمًا؛ حتى تتمكَّن من الوصول إلى بياناتك في أيّ وقت ومن أيّ مكان.

انْتَبِه!

قاعدة 3-2-1

يُقصَد بها إنشاء 3 نُسَخ مختلفة من البيانات لوَضْعها على نوعين مختلفين من وحدات التَّخزين والاحتفاظ بنسخة واحدة خارج الموقع، وهناك عدَّة طُرُق لذلك:

- استخدام مُحرِّك أقراص ثابت خارجيّ.
- استخدام برنامج نَسْخ احتياطيّ تابِع لجهة خارجيَّة، مثل البرامج السَّحابيَّة.
- نَسْخ الملفَّات يدويًّا.

انْتَبِه!

تعريف البرمجيّات الضارة

مصطلح شامل يَصِف أيّ برنامج أو تعليمات برمجيّة ضارّة تَضُرّ بالأنظمة، فهي تسعى عن عَمْد إلى غَزْو أجهزة الحاسوب وأنظمتها والشّبكات والأجهزة اللّوحيّة والأجهزة المحمولة بهدف إتلافها أو تعطيلها، وذلك غالبًا عن طريق التّحكُّم الجزئيّ في عمليّات الجهاز.

انْتَبِه!

الوصول غير المُصرَّح به (غير القانونيّ)

هو عمليَّة الدُّخول إلى موارد الحاسوب دون إذْنٍ، ويمكن أن يكون نظامًا أو شبكةً أو برنامجًا أو بياناتٍ، وعادةً ما يتمّ ارتكاب الوصول غير المُصرَّح به من قِبل المُتسلِّلين، وأحيانًا المُستخدِمين غير المُتعمِّدين، فيمكن لأيّ شخص لديه إمكانيَّة الوصول بالفعل إلى النِّظام أن يَعْثُر بطريق الخطأ على ملفَّات غير آمِنة لم تكن مُخصَّصة للمُعاينة.

كيفيّة الحفاظ على البيانات آمِنة

انْتَبِه!

1. اسْتَخدِم كلمات مرور قويّة وغيّرها بين الحين والآخر.
2. تَجَنَّب استخدام نفس كلمة المرور لحسابات متعدّدة.
3. تَجَنَّب كتابة كلمات المرور الخاصّة بك في أيّ مكان.
4. المصادقة مُتعدّدة العوامل.
5. كُن حَذِرًا عند مشاركة المعلومات الشّخصيّة.
6. الحد من مشاركة البيانات الشّخصيّة عَبْر منصّات التّواصُل الاجتماعيّ.
7. اسْتَخدِم برامج مُكافَحَة الفيروسات.
8. إغلاق الحسابات غير المُستخدَمة على الإنترنت.
9. حافِظ على تحديث الأنظمة والبرامج.
10. كُن حَذِرًا من خدمة Wi-Fi المجانيّة.

انْتَبِه!

سرقة البيانات

هي نَقْل أو تَخْزين غير قانونيّ للمعلومات الشَّخصيَّة أو السِّرِّيَّة أو الماليَّة، ويمكن أن يشمل ذلك كلمات المرور أو التَّعليمات البرمجيَّة أو الخوارزميَّات البرمجيَّة والعمليَّات أو التِّقنيَّات الخاصَّة، وتُمثِّل انتهاكًا خطيرًا للأمان والخصوصيَّة.

انْتَبِه!

برمجيّات الفِدْيَة Ransomware

عبارة عن برمجيّات ضارّة مُصمَّمة لمَنْع المُستخدِم أو المؤسّسة من الوصول إلى الملفّات الموجودة على أجهزة الحاسوب الخاصّة بهم، للمُطالَبَة بدَفْع فِدْيَة مقابل استعادة الوصول إلى ملفّاتهم.

انْتَبِه!

أمن المعلومات Information Security

يُقصَد به الوسائل والأدوات والإجراءات اللَّازم توفيرها لضمان حماية المعلومات من الأخطار الدَّاخليَّة والخارجيَّة، وهو العِلْم الذي يَدْرُس كيفيَّة توفير تدابير حماية سرِّيَّة وسالمة للمعلومات وكيفيَّة مُكَافَحَة الاعتداء عليها.

انْتَبِه!

أمن الشَّبكات

هو جزء من منظومة أمن المعلومات التي تقوم على حماية استخدام الشَّبكة وسلامتها، ومِن ثَمَّ سلامة عمليَّات نَقْل وتَبادُل البيانات، ويشمل هذا المجال كلًّا من تكنولوجيا الأجهزة والتَّطبيقات، ويَستهدِف مجموعةً مُتنوِّعةً من التَّهديدات ويَمْنَعُها من الدُّخول إلى شبكتك أو من الانتشار.


الإسكتشات

أبرز المَخاطِر الرَّقميَّة التي تواجه الأجهزة الرَّقميَّة (الحواسيب، الهواتف الذَّكيَّة، الأجهزة اللَّوحيَّة)

01 تَسَرُّب البيانات

02 تزوير الشَّبكة

03 هجمات التَّصيُّد الاحتياليّ

04 برمجيَّات التجسس

كيفيَّة عمل بَرْمَجيَّات الفِدْيَة

هناك ثلاث مراحل أساسيَّة تَمُرّ بها هذه العمليَّة

- ناقلات العدوى والتَّوزيع
- تشفير البيانات
- طَلَب الفِدْيَة

كيف يمكن الحماية من برمجيَّات الفِدْيَة؟

1. التَّوعية والتَّأهيل والتَّدريب على مفاهيم الأمن السِّيبرانيّ والسَّلامة الرَّقميَّة.
2. النَّسْخ الاحتياطيّ المستمرّ للبيانات.
3. تصحيح الثَّغرات في الأنظمة التي لم تُصحَّح بعد.
4. تُعَدّ مصادقة المُستخدِم وسيلةً مهمَّةً لمَنْع المُهاجِم من الاستفادة من كلمة المرور التي تمّ تخمينها أو سرقتها.
5. تقليل سَطْح الهجوم، ويتمّ ذلك عن طريق معالَجة الآتي:

- رسائل التَّصيُّد.
- نقاط الضَّعف غير المُصحَّحة.
- حلول الوصول عن بُعْد.
- البَرمَجيَّات الضَّارَّة للأجهزة الذَّكيَّة.


كيف تُخَفِّف من عدوى برمجيَّات الفِدْيَة النَّشطة؟
عَزل الجهاز
اترُك الحاسوب قَيد التَّشغيل
إنشاء نسخة احتياطيَّة من الملفَّات
المَسح والاستعادة عبر تثبيت نظـام التَّشغيل لضـمان إزالة البَرْمَجيَّات الضَّارَّة بالكامل من الجهاز
اطلُب المساعدة من شخص مُتخصِّص
التَّحقُّق من وجود أدوات فكّ التَّشفير

كيف تحدث سرقة البيانات؟

تحدث من خلال مجموعة مُتنوِّعة من الوسائل

1. **الهندسة الاجتماعيَّة.**
2. **كلمات المرور الضَّعيفة.**
3. **نقاط ضعف النِّظام** (الثَّغرات الأمنيَّة).
4. **التَّهديدات الدَّاخليَّة** من قِبل بعض المُوظَّفين الذين يعملون في مؤسَّسة ما للوصول إلى المعلومات الشَّخصيَّة للعملاء واستغلالها.
5. **خطأ بشريّ.**
6. **تثبيت البرامج من مواقع غير موثوقة.**
7. **سرقة الأجهزة الإلكترونيَّة أو ضياعها.**
8. **المعلومات المتاحة للجمهور.**

نصائح لاكتشاف الدُّخول غير المُصرَّح به ومَنْعه

1. وَضْع سياسة كلمة مرور قويَّة ومُعقَّدة وتغييرها بين الحين والآخر.
2. التَّذكير والفحوص المُنتظِمة بشأن الممارسات الأمنيَّة عبر التَّدريب.
3. تقليل عدد الأجهزة التي يمكنها الوصول إلى البيانات الحسَّاسة.
4. تأمين جميع نقاط النِّهاية عبر تثبيت برنامج مُكَافَحَة الفيروسات على كلّ نقطة نهاية؛ لاكْتِشَاف البَرْمَجيَّات الضَّارَّة وإزالتها.

كيف يمكنني معرفة ما إذا كان جهازي مصابًا بعدوى البرمجيّات الضّارّة؟

- بَطْء جهاز الحاسوب الخاصّ بك.
- ظهور الإعلانات المُزعجة على الشّاشة.
- تَعطُّل نظام التّشغيل، ويأتي هذا على شكل تجميد أو شاشة الموت الزّرقاء (BSOD)، ويحدث هذا الأخير على أنظمة Windows.
- فقدانٌ غامضٌ لمساحة القُرْص.
- زيادةٌ غريبةٌ في نشاط الإنترنت لنظامك.
- تَغَيُّر إعدادات المُتصفِّح الخاصّ بك.
- تَوقُّف برنامج مُكَافَحَة الفيروسات الخاصّ بك عن العمل.
- فقدان إمكانيّة الوصول إلى ملفّاتك أو جهاز الحاسوب بأكمله.

كيفيَّـة إزالـة البرمجيَّـات الضَّـارَّة

1

ثَبِّت وحَمِّل برنامجًا جيِّدًا لمُكافَحَة البَرْمَجيَّات الضَّارَّة.

2

أجْرِ فَحْصًا باستخدام برنامجك الجديد.

3

غَيِّر جميع كلمات المرور الخاصَّة بك.

أهمِّيَّة حماية كلمة المرور

هي خطّ الدِّفاع الأوَّل ضدّ الوصول غير المُصرَّح به إلى الحسابات والأجهزة والملفَّات عبر الإنترنت، وتُساعِد كلمات المرور القويَّة على حماية البيانات من العناصر السيئة والبرمجيَّات الضارة، فكلَّما كانت كلمة المرور أقوى؛ زادت حماية المعلومات.


إرشادات عامَّة
لإنشاء كلمات
مرور قويَّة
1
اسْتَخدِم ما لا يقلّ
عن 12 حرفًا.
2
اسْتَخدِم مزيجًا من الحروف
والأرقام والرُّموز.
3
اسْتَخدِم حرفًا كبيرًا
واحدًا على الأقلّ.
4
اسْتَخدِم كلمة مرور مختلفة
لكلّ حساب من حساباتك.
5
اسْتَخدِم كلمات غير مألوفة وغير
عاديَّة، مثل كلمات الأغاني أو
الاقتباسات أو العبارات الشَّائعة.

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency